The Honorable James L. Robart

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. VOLODYMYR KVASHUK, Defendant.	NO. CR19-143JLR GOVERNMENT'S TRIAL BRIEF

The United States of America, by and through Brian T. Moran, United States Attorney for the Western District of Washington, and Michael Dion and Siddharth Velamoor, Assistant United States Attorneys for said District, files this Trial Brief. Trial is scheduled for February 18, 2020.

I. BACKGROUND

The Second Superseding Indictment charges Volodymyr Kvashuk with access device fraud (Count 1), unauthorized access to a protected computer (Count 2), mail fraud (Count 3), wire fraud (Counts 4-8), making and subscribing to false tax returns (Counts 9-10), money laundering (Counts 11-16), and aggravated identity theft (Counts 17-18). *See* 2d Superseding Indictment ("SSI"), Dkt. 61. The charges arise out of Kvashuk's embezzlement of approximately $10 million in digital currency from Microsoft's online store.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

A. The Offense Conduct

As set out in the government's previous submissions,[1] Kvashuk is a former software engineer at Microsoft Corporation ("Microsoft"). Microsoft is a company based in Redmond that sells and licenses computer software and hardware, remote computing services, and other information-technology products. Kvashuk worked as an outside contractor to Microsoft between August 2016 and October 2017. He returned as a full-time employee in December 2017 and remained at the company until his termination in June 2018. Kvashuk's final annual salary at Microsoft was approximately $116,000.

Between August 2016 and June 2018, Kvashuk was a member of Microsoft's Universal Store Team ("UST"). SSI ¶ 8. UST supported the Microsoft online store, an internet-accessible Microsoft digital marketplace on which people can buy physical items (e.g., laptops, video-game consoles, tablets, and phones) and digital products (e.g., software). *Id.* ¶¶ 6-8. UST wrote the programming code that operates the online store, and tested that code to ensure that it worked as intended. *Id.* ¶ 8.

To simulate the customer experience on the Microsoft online store, UST members took some of the steps that an ordinary customer would take. For instance, UST members set up accounts on the Microsoft online store, browsed the online store's offerings, added items to digital shopping carts, and gifted items to other online-store accounts. *See id.* ¶¶ 7, 9. UST members registered these "test accounts" using digital credentials—namely, email addresses, usernames, and passwords—which were created specifically for the purpose of testing. *See id.* ¶ 9. Microsoft also gave UST members artificial payment devices (i.e., phony credit cards), named "Test in Production" ("TIP") cards, that could be used to "make payment" for products purchased using test accounts. *Id.*

[1] *See* Memo. In Support of Mot. for Detention, Dkt. 9; Opp. to Mtn. for Review, Dkt. 33; Opp. to Mot. to Suppress, Dkt. 67; Opp. to Mot. to Dismiss, Dkt. 66.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Kvashuk had access to the usernames and passwords for other employees' test accounts. Specifically, Kvashuk's former supervisor and colleague both will testify that UST members browsed and interacted with the Microsoft online store in the same way that ordinary customers would. If, in the process of conducting that form of testing, they discovered a "bug"—*i.e.*, a feature of the online store that did not operate as intended—then they used a program named "Fiddler" to track the exact steps that caused the bug to arise. However, because Fiddler tracked *all* of the relevant actions, it also tracked the username and password for the UST members' test accounts. Thus, the reports that Fiddler generated sometimes included the UST members' login information, which Kvashuk could access on the Microsoft network.

Although the testing program was designed to simulate almost all aspects of the customer experience, it did not simulate the *entire* customer experience. Specifically, whereas actual customers receive products in the mail after purchasing them on the online store, the testing program was designed to block the delivery of physical goods purchased by test accounts. *Id.* ¶ 10. Furthermore, test accounts also were generally exempted from certain anti-fraud features to which ordinary customer accounts are subject.

1. *Kvashuk's Theft From Microsoft*

Kvashuk's criminal scheme involved the use of his and other UST members' test accounts to purchase digital gift cards from the Microsoft online store. While Microsoft blocked the delivery of physical goods (e.g., laptops) purchased by test accounts, no such safeguards prevented the delivery of digital gift cards purchased by test accounts. Those digital gift cards, which Microsoft refers to as "Currency Stored Value" or "CSV," are a form of digital currency that anybody can use in order to purchase items on the Microsoft online store. *See id.* ¶ 10. To redeem the value of a digital gift card, a purchaser must use a 25-digit alphanumeric code that Microsoft generates at the time the digital gift card is purchased.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The code is displayed as five (5) sets of five (5) letters and numbers and, therefore, is typically referred to as a "5X5 code." Microsoft typically provides the gift card's purchaser with the 5X5 code at the time of purchase, both by displaying the code on the purchaser's screen and by emailing the code to the purchaser's email account.

Kvashuk knew he was not supposed to misuse test accounts to embezzle CSV for his personal benefit. Microsoft witnesses will testify that the test accounts were to be used only for testing purposes, and not for personal gain. In violation of these rules, Kvashuk purchased over $10 million in CSV between 2017 and 2018. He used a small amount of that CSV to purchase physical products from the Microsoft online store, and re-sold the vast majority of the CSV on an online marketplace called Paxful.

Kvashuk used four UST test accounts to purchase CSV:

- **The "vokvas" account**: The test account assigned to Kvashuk had the username "v-vokvas," which was derived from his first and last name – i.e., "**vo**[lodymyr]**kvas**[huk]." In the approximate time period April 2017 to October 2017, the vokvas account purchased over $10,000 in CSV. *Id.* ¶ 12. In May 2018, Microsoft investigators interviewed Kvashuk in a partially recorded interview. During that interview, Kvashuk admitted that he used the vokvas account to purchase CSV, and that he used some of the CSV to rent movies from Microsoft. (Kvashuk omitted, however, that he had used other test accounts to purchase millions of dollars in CSV, which he re-sold on secondary marketplaces for Bitcoin.)
- **The "avestu" account**: The "avestu" account was a test account that was not controlled by any particular UST member. (The account had the ability to run automated tests on the Microsoft online store.) Between November 2017 and March 2018, Kvashuk used the avestu account to purchase approximately $1.6 million in CSV between November 2017 and March 2018, excluding amounts that Microsoft "blacklisted" (by making unavailable for redemption) after learning about the fraud.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

- **The "swfe2eauto" account**: The "swfe2auto" account was assigned to "A.C.," a UST employee who will testify that he did not authorize Kvashuk to use the account. Between November 2017 and March 2018, Kvashuk used the swfe2eauto account top purchase approximately $6.04 million in CSV, excluding amounts that Microsoft "blacklisted" (by making unavailable for redemption) after learning about the fraud.
- **The "zabeerj2" account**: The "zabeerj2" account was assigned to "Z.J.," a UST employee who will testify that he did not authorize Kvashuk to use the account. In March 2018 alone, the zabeerj2 account purchased approximately $643,000 in CSV, excluding amounts that Microsoft "blacklisted" (by making unavailable for redemption) after learning about the fraud.

Overwhelming evidence establishes that Kvashuk used these accounts to purchase CSV without authorization. Records produced by Google regarding the internet and search history for Kvashuk's personal email account show the genesis of his fraud scheme in February 2017, before he began purchasing CSV. As the search history shows, Kvashuk sought information about "cash for gift card," visited websites that allowed him to "Sell Gift Cards for Cash Online." Kvashuk also sought information about how to conceal his online activities, by searching for "hide my ass web," "proxy" servers, and virtual private network providers.

In two interviews with Microsoft investigators in May 2018, Kvashuk admitted using the v-vokvas account to purchase CSV (though he omitted his use of the other test accounts for the same unauthorized purpose). Microsoft records also showed that some of the CSV purchased by the v-vokvas account was redeemed (*i.e.*, used for the purchase of goods and services from the Microsoft online store) by other store accounts connected to Kvashuk.[2]

[2] CSV purchased by one Microsoft online store account can be redeemed by a different online store account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Kvashuk admitted to Microsoft investigators that he used some of the CSV purchased by v-vokvas to rent movies and to purchase other items using an account that he registered under the email address safirion@outlook.com. Microsoft separately discovered that two other store accounts registered under xidijenizo@axsup.net and pikimajado@tinoza.org redeemed some of the CSV purchased by v-vokvas to order digital graphics cards. Agents could not find any records for those email address, which suggested that they were "disposable" email accounts that Kvashuk used for the sole purpose of registering store accounts.

When ordering graphics cards, both accounts provided billing information that matched the street address for the apartment building that Kvashuk lived in at the time of those purchases, which was an apartment building named Norman Arms in the University of Washington District. However, the accounts' billing information used a non-existent apartment number and a fictitious name ("Greg Shikor"). Federal Express has provided records confirming that the graphics cards purchased by xidijenizo were delivered to the apartment building, and that the package listed a recipient named "Grigor Shikor." As Kvashuk's former apartment manager will explain, nobody named "Grigor Shikor" has ever lived in the building. Mailed packages were often left in a common area of the apartment building, where they could be picked up by the building's residents.[3]

The evidence of Kvashuk's use of the other test accounts is also clear. In July 2019, law-enforcement agents searched Kvashuk's lakefront home in Renton, which Kvashuk purchased using proceeds from his scheme. Inside the home, agents found numerous records that incriminated Kvashuk, such as multiple versions of the document excerpted below, which appears to show Kvashuk's working notes from the fraud:

[3] When first interviewed by Microsoft's investigators, Kvashuk disclaimed knowledge of the delivery to "Grigor Shikor." In a subsequent interview, Kvashuk insisted that he had asked his landlord about the delivery and about the availability of surveillance footage from the mailroom that could help identify "Grigor Shikor." In truth, Kvashuk had no such conversation with his apartment manager.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ï»¿ms accounts
pikimajado@tinoza.org
xidijenizo@axsup.net
jasufo@ethersports.org
pavabahok@asorent.com
Aq1Sw2De3

xyfqgpimb@emltmp.com
Aq!sw2De#

1tm3now
srjg0u3cc6

13jzbpR2oM4vbVRseQnm9ttEo733s4KQt4 coinbase
1H4ecvMY8zLhu3uKaKTis6cwoRjZo23iUF blockchain

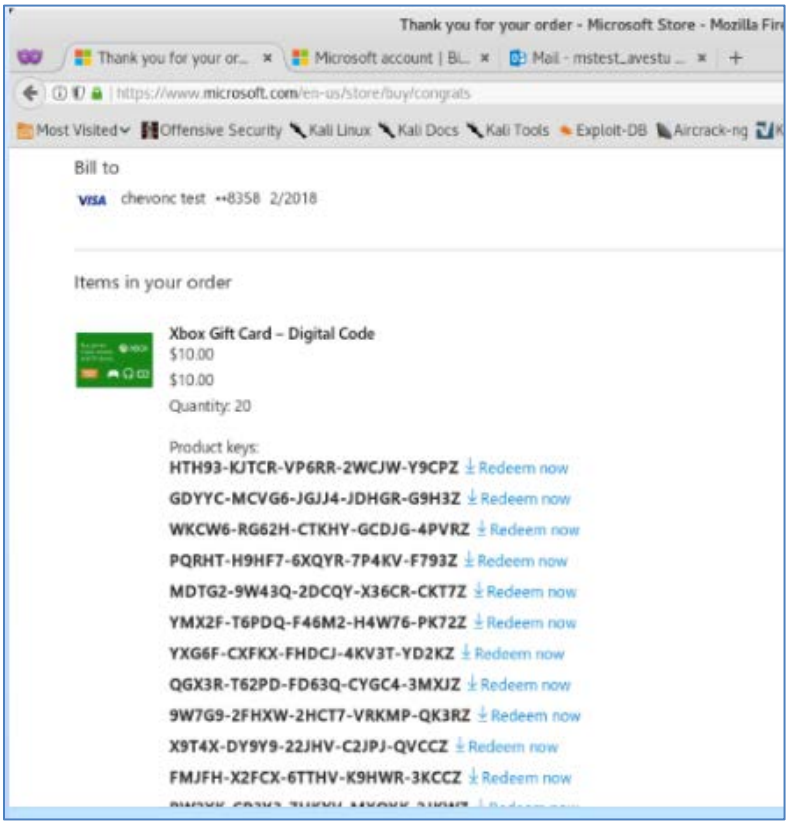
10k usd
41x50usd
138x50EUR
100x50GBP
50x40GBP

The working notes refer to multiple aspects of the fraud, including the pikimajado and xidijenizo accounts, gift-card denominations, and Coinbase (a cryptocurrency exchange into which Kvashuk received Bitcoin that he purchased using gift cards). The working notes also referred to the login names and passwords for two of the test accounts that had been assigned to other UST members, and which Kvashuk used to purchase CSV:

mstest_avestu@outlook.com || Monkey@888 ++++
mstest_sfwe2eauto@outlook.com || sfwe2eauto123 +++

In addition to Kvashuk's working notes, agents also found screenshots (i.e., a screen-capture that Kvashuk created of an image shown on his monitor) of Microsoft online store order confirmations for 5X5 codes. One of the screenshots is shown below:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



The screenshot shows multiple 5X5 codes that Kvashuk purchased using the avestu test account, each worth $10.00. The screenshot also shows that, at the time Kvashuk made this purchase, his internet browser was logged into the email account associated with the avestu account (as shown by the third tab on the top of the screen labeled "Mail – mstest_avestu"). As the case agent will explain at trial, a number of the confirmation emails for CSV purchases that otherwise should have been in the test accounts' email addresses were missing, which Kvashuk could have accomplished by deleting the confirmation emails at the time that he purchased the codes.

In addition to finding screenshots of order confirmations, agents also found spreadsheets and other documents on Kvashuk's digital devices that tracked thousands of 5X5 codes that had been purchased using the test accounts. One example of Kvashuk's tracking spreadsheets is shown below. As it makes clear, Kvashuk organized CSV codes by amount (e.g., $100 or $50):

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

	A	B	C	D	E	F
1	#	box Digital Gift Card: $100.00		Xbox$100		xbox50
2	1	GGWTM-FHH7V-J39MV-KP2JV-7R7PZ Redeem now	1	609	1	H6M77-PQ9W2-F4JF2-MPGYR-FD7DZ Redeem now
3	2	47TCK-RHT47-KM26H-2T33M-QF6RZ Redeem now	1	60900	2	D4362-FKK6H-XFJ66-K2MWR-VT2GZ Redeem now
4	3	4WFPM-FCHPG-FPXWJ-HG6WR-PF6JZ Redeem now	1		3	DK7XK-X6FJ4-DP3PG-P9W3C-XPGXZ Redeem now
5	4	XKF67-TG7TF-GMM9D-YH7KD-C39DZ Redeem now	1		4	JDRJX-7Y3J4-FWMFM-YGCX2-QMDDZ Redeem now
6	5	KPK6P-9KPHR-XMG34-76DJY-YXV2Z Redeem now	1		5	2YYHQ-WDYYQ-G3RM7-2DF46-94GKZ Redeem now
7	6	9Y7DY-DQGVT-QM7W7-XQRC4-X4C7Z Redeem now	1		6	744YJ-226HQ-WFMF6-DV2RC-YD69Z Redeem now
8	7	M2M76-3P99M-CJRTC-79PG3-W9P6Z Redeem now	1		7	KDQ6F-YRC9M-QW6K9-R2KTV-P6VVZ Redeem now
9	8	VT667-3K94Y-6PHPQ-7J2GD-Y7WXZ Redeem now	1		8	MHCF6-WMFTK-39HRD-DVRG4-D72JZ Redeem now
10	9	F4M93-YQ6T7-6DJ94-PG2V9-K76CZ Redeem now	1		9	CPW9W-JCVCP-PT3CP-PCQMW-R7P4Z Redeem now
11	10	764HT-V23CD-DQTPP-3R36F-6KK9Z Redeem now	1		10	2QMR9-7T9MT-TP7DH-XRKCG-7GTTZ Redeem now
12	11	MTD49-TTHTD-VFFHX-2QY43-DVVKZ Redeem now	1		11	6DPRT-GT37V-TP2DT-TKWTJ-4PYGZ Redeem now
13	12	HWMWQ-MPGQ3-G7GWQ-36JDV-3QCPZ Redeem n	1		12	7PFWX-M2DCH-37FR2-JW3Q4-PK29Z Redeem now
14	13	Y7MCG-6CM4Y-XWYKH-W44QV-DC9XZ Redeem now	1		13	C6QC7-GW6J6-T32XM-K4477-QQMTZ Redeem now
15	14	VWCCV-WPGHF-9RJG2-XDGTW-CXVHZ Redeem now	1		14	HYX9V-KQRD4-2C34R-6HMKT-QTYWZ Redeem now
16	15	WY23K-QDMRD-JPCG2-JGRXD-69MVZ Redeem now	1		15	4WGXT-DKDTX-CWJ2V-DPYQP-4JDRZ Redeem now
17	16	CMHVM-TC6HX-HW9KR-VCYXQ-W9Y2Z Redeem now	1		16	G3G7X-F32DQ-DFWDG-FGGDJ-W3HGZ Redeem now
18	17	JKYJH-H7HHC-3Q3QQ-PHQFF-KXHJZ Redeem now	1		17	HGV6V-RT7PF-HR9TC-DD994-QPQFZ Redeem now
19	18	RYWG7-PVWX2-774XK-93P3R-VTVFZ Redeem now	1		18	VMGHY-7C2QV-42YXD-DJR2V-D262Z Redeem now
20	19	7WDPW-RYHV9-GJDWP-93DFC-DKM2Z Redeem now	1		19	2VGXK-TGYTJ-42TJF-MHCPF-H9YDZ Redeem now
21	20	RVDHC-RRGP9-HPWGV-7MCY3-9DT3Z Redeem now	1		20	DQ9DX-3VDFY-GTFWM-VC6WR-V22MZ Redeem now
22	21	7CJRQ-RDM7T-9T7H4-F6FPM-6WGXZ Redeem now	1		21	FJ2M4-2YQM3-Y4P29-YV2G7-T736Z Redeem now
23	22	T26RM-VPVHM-6PR6F-KVFRF-G34FZ Redeem now	1		22	M62H2-F2GVT-J97RR-FPW36-GG6HZ Redeem now
24	23	DKFFD-JWQCQ-34YTR-H37TV-CKRXZ Redeem now	1		23	Q6VQD-FPCVM-MM92Q-9PW7W-PWX2Z Redeem now
25	24	9QRFG-YQHGT-CXQCP-KGX6F-DXRPZ Redeem now	1		24	Y322J-KQX2F-WRXG2-47T46-JV3MZ Redeem now
26	25	HWDJY-FHQMH-CMCQC-7PGP4-HGQRZ Redeem now	1		25	67K6R-79P4M-J9M7H-KHHKP-MQ6FZ Redeem now
27	26	2KJKW-6RKDG-DM7DT-FKGQC-2GF2Z Redeem now	1		26	XJF9H-6X36Y-4CPDY-7K2RC-C37TZ Redeem now
28	27	6MTJY-G2QJC-6C2HR-6JJKM-JRFRZ Redeem now	1		27	JHQ2H-JDFK2-6D7TG-9HV2T-MH7GZ Redeem now
29	28	T36QW-TWCDM-HH6TF-WTWQC-TVM7Z Redeem now	1		28	77R96-WMGRW-3PHMH-24Y9Y-C6PXZ Redeem now
30	29	R4FMV-2WWVX-9V4FP-T6MPY-TDFGZ Redeem now	1		29	KWKVK-6QF4T-MGDP6-FPKY2-KWCJZ Redeem now
31	30	JGKJJ-HKJD2-XF9D4-Q3YHG-27CJZ Redeem now	1		30	36329-MVFVW-33JCP-RWHRV-V6DMZ Redeem now
32	31	7MHPF-3K9Q6-Q4C9V-XY6QP-TYVQZ Redeem now	1		31	T7XJD-CGVYH-XQR77-JC3J4-J6JXZ Redeem now
33	32	DF4DT-43VYJ-GW6W4-HKM6W-7TMTZ Redeem now	1		32	FQG27-HGCPR-C7YGD-YVMFX-Y3K6Z Redeem now
34	33	QHT32-RRJ2X-934CY-QYG9Q-HF72Z Redeem now	1		33	MVR6P-DK6DR-XYKVV-KTQCT-FMYVZ Redeem now
35	34	39RY9-FJVJ6-W4GWD-KGKYF-F6M4Z Redeem now	1		34	PV26C-WX4XG-JDKHG-DKK27-7FPCZ Redeem now
36	35	3H2HP-FCH3P-2D27X-RGCM7-3VX7Z Redeem now	1		35	KKC9P-HMHPF-2KK79-4RWQ6-Y3F6Z Redeem now
37	36	3Y7TT-K3R27-JX4JC-63QMJ-KY6PZ Redeem now	1		36	C6GX2-4VQM2-7JFTJ-9V9QR-6G4RZ Redeem now

Agents also found a computer program on Kvashuk's digital device named "Purchase Test," which used the zabeerj2 username and password in order to log into the Microsoft online store and purchase CSV. At trial, the government will offer a video created by a forensic examiner who ran the program on a forensic image of Kvashuk's computer. As reflected in the screenshots from the video below, the program required Kvashuk to select both the number of gift cards that he wished to purchase, as well as the gift card denominations. (Because Kvashuk's computer was not connected to the internet at the time the forensic examiner ran the program, the program could not connect to the Microsoft online store and complete the purchase.)

//

//

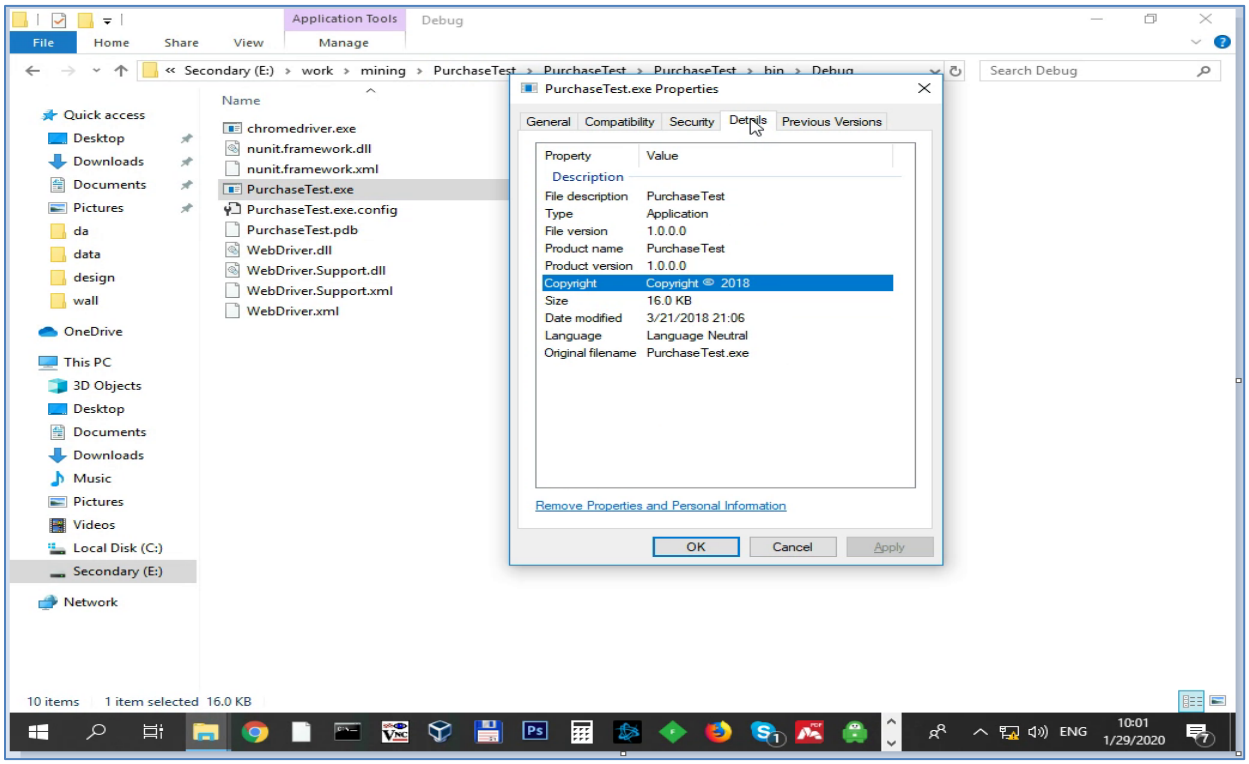
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Screenshot 1: Excerpt of Script for "Purchase Test" Program, Showing Use of zabeerj2 Account Credentials

```
string userName = "mstest_zabeerj2@outlook.com";
string passwrod = "$tore123";
IWebDriver driver;

//checkIfLogedIn(), login(), checkIfCartEmpty(), emptyCart(), addItemsToCart(itemUrl), changeQuantity(), proceedToCheckout() check if
//quantity 100 if 100 then checkout if not then changeQuantity(),
//selectPI() if PI needs to be selected, select PI and address, wait for button, click buy, exportCodes()
```

Screenshot 2: Icon and Properties for "Purchase Test" Program

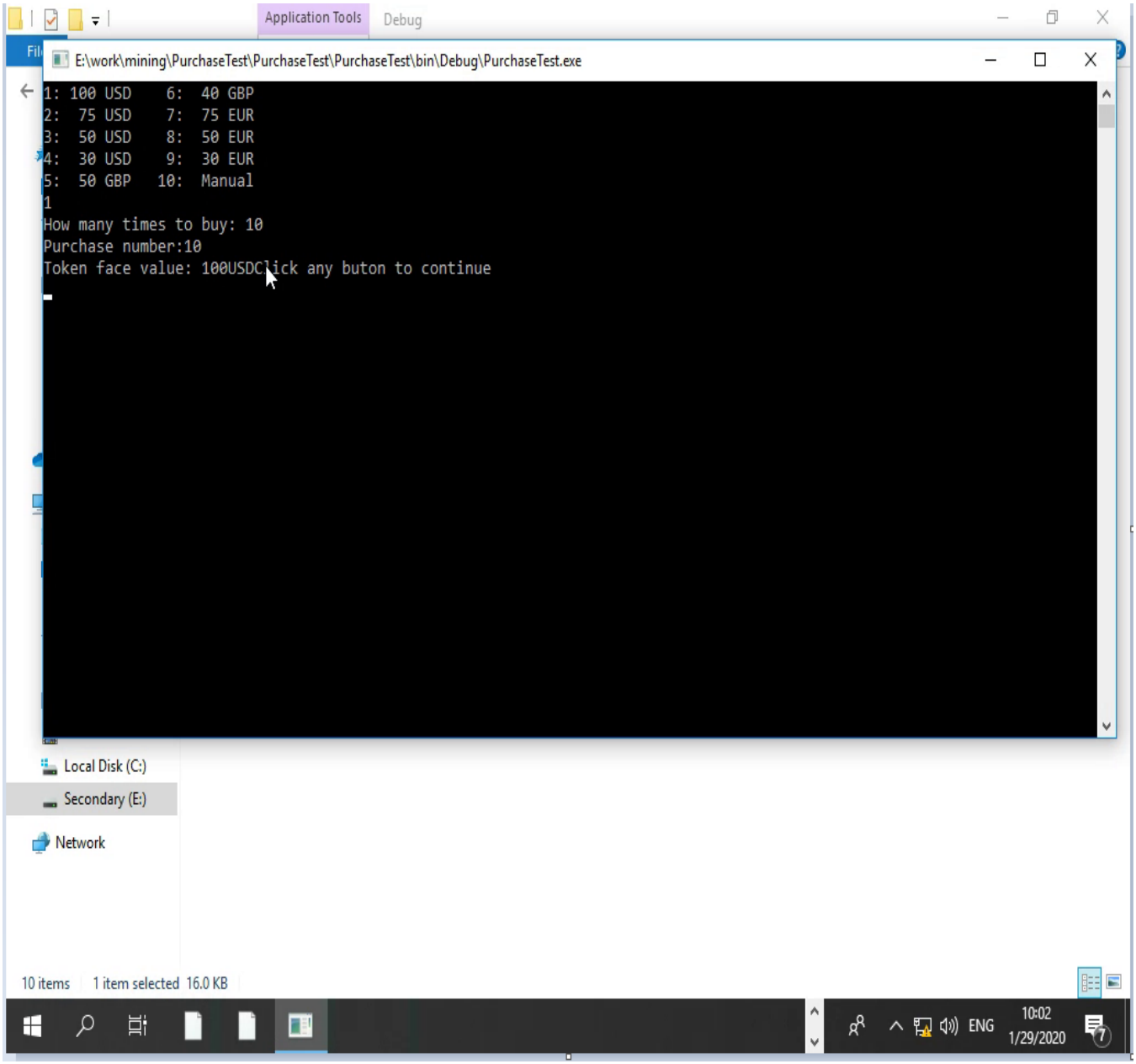


//

//

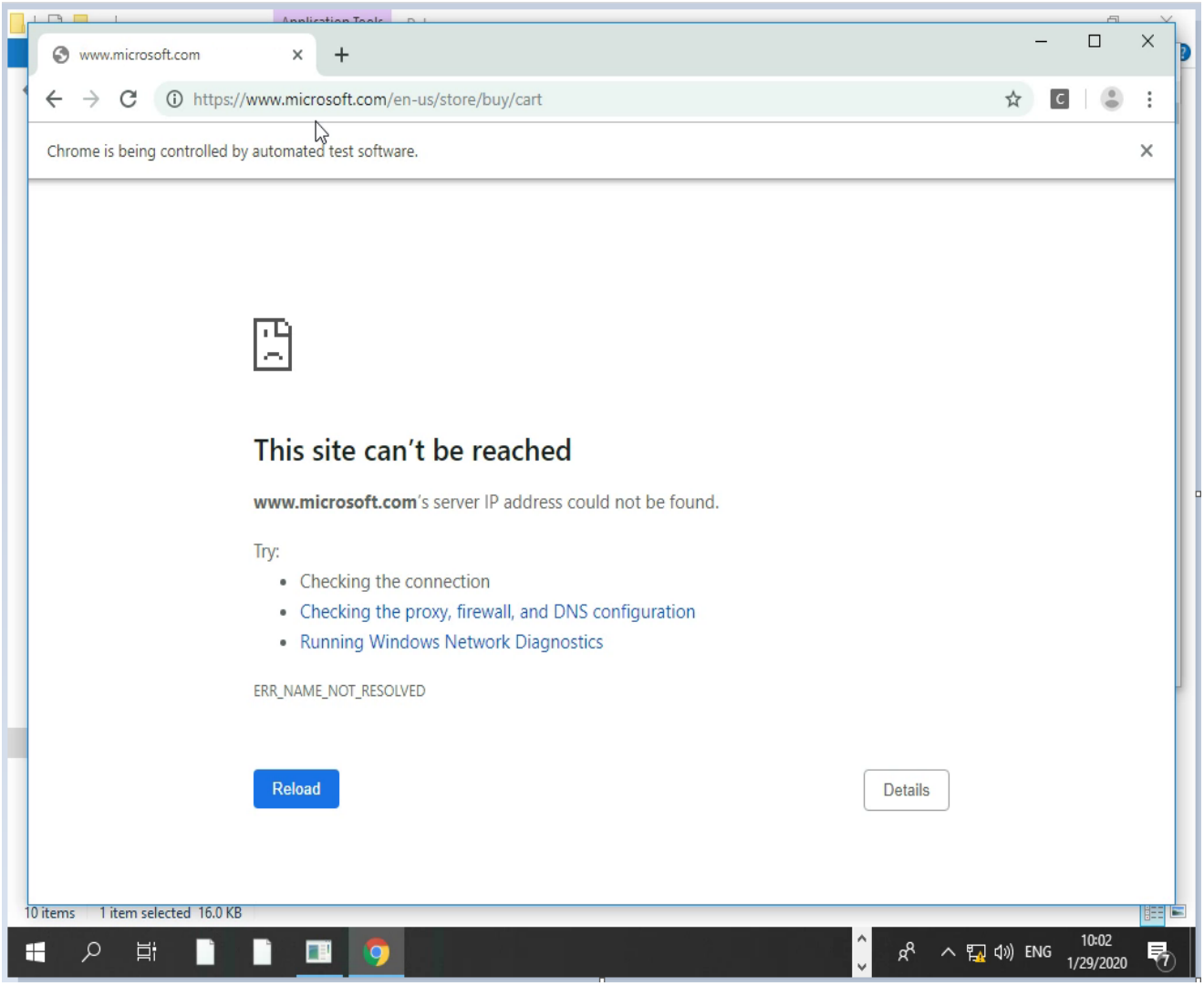
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Screenshot 3: Operation of "Purchase Test" Program, Which Asks User to Designate Gift Card Denominations and Currencies, "How many times to buy," "Purchase number," and "Token face value"



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Screenshot 4: Screenshot of "PurcahseTest" Program Attempting to Connect to "www.microsoft.com/en-us/store/buy/cart"



2. Kvashuk's re-sale of 5X5 codes obtained through the test accounts

Records produced by paxful.com, an online marketplace on which people can purchase cryptocurrency using gift cards, show that Kvashuk registered an account on the website under the name "Grizzled" and the email address grizzled@protonmail.com. "Grizzled" was the username on a computer found in Kvashuk's residence, and grizzled@protonmail.com was the same email address that Kvashuk provided when registering an account on the cryptocurrency exchange Coinbase.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Between December 2017 and March 2018, Kvashuk's Paxful account traded approximately $7.8 million in gift cards for Bitcoin, the cryptocurrency. Paxful produced online "chats" in which Kvashuk exchanged messages with others about potential trades. In early trades (when Kvashuk was not yet selling CSV but instead was tinkering with the platform), Kvashuk told others that his name was "Volodymyr Kvashuk" and told them to send funds to a PayPal account in his real name. Once Kvashuk familiarized himself with the platform and started selling large quantities of CSV, the chats followed a familiar pattern, illustrated below:

Trade vp1yEPwkX1q

ID	12522802
Offer Owner	rpstenangam
Payment method	Xbox Gift Card
Label	INSTANT REDEEM
Offer type	2
Offer limits	50.00 - 1000.00 US Dollar
Payment window (minutes)	120
Insta-funded	1
Margin	90.00
Trade started by	Grizzled
BTC	0.09292034
Rate	11433.39 USD / BTC
Paid	1

At the beginning of the chat, Kvashuk (under the name "Grizzled") "started" a trade, in which he used the payment method "Xbox Gift Card" to purchase "BTC" or Bitcoin at a specified rate. Upon agreeing to the trade, Kvashuk sent dozens of gift card codes to his counterparty:

2017-12-04 06:19:11	Grizzled	1 HK299-77M2D-7XK9X-2YCRC-X7PGZ 2 7P64F-YTQ34-HVVRJ-CQGPQ-W3HDZ 3 6MGYV-DDC22-D6T7H-XRTKF-Y6G3Z 4 P3THG-WW6W7-JX2RV-PM4DY-F74CZ 5 Y976X-F34CY-GTW3X-HQDCF-W9KMZ 6 H2GCM-KJVHD-WJX4V-7KGRK-HW4XZ 7 FX6HJ-DJ4F6-DFYDR-R24MG-GDPPZ 8 479WF-PM77V-CHCC3-FHWV4-96FKZ 9 JXWX4-M3XRV-93C4R-FYJFG-GCMFZ 10 7HQDH-9DC6W-DCFRJ-MFC3K-YGDTZ 11 67JR9-DPXPP-XXVKJ-PTCG4-YH49Z 12 PDWVJ-T7WXT-924JK-97PV4-V3RTZ 13 HM2M4-XP6MD-Q3P6V-9MWM9-3CMHZ 14 F6FQM-WGPMQ-9HVVJ-KFF9F-63V3Z 15 RWJRT-46YKG-YHM4J-677XM-JGMHZ 16 P3M2W-WJD67-64FGP-J4R97-M3CWZ 17 WYX2D-JY6C7-4742Y-VR767-2R9KZ 18 2DQ6R-6FW4R-JTMC9-9YJX3-6RVRZ 19 CYMFV-6GYRX-G3PGK-2J7VM-7CF6Z 20 GGMHX-JQ2VX-9VCRG-T9P2R-4H62Z 21 296KX-674GX-RPTF9-J34WX-7C67Z 22 J66PJ-CKRV9-24VVV-7KR36-DDJYZ 23 VRMQR-QMHPX-KXW4H-YVQR6-TQTCZ 24 KVY32-93DKH-TGCM6-HVVP7-3F47Z 25 GDPDG-KCDD4-RQQXM-Y2FW7-MHXRZ 26 72V7P-67HQY-HQWQ7-39TWQ-4JC9Z 27 MFT99-YVCXF-9KPTR-PY6MR-TD7FZ 28 GRMPK-GRXQX-YWPKM-WF72D-6D4PZ 29 WC2TX-H2RT9-M73M9-VXCH9-6DGXZ 30 4VPCY-DD4C9-R2WJM-GCTP9-K3PVZ 31 26KYF-FF6GJ-6M733-97X2W-WW74Z 32 F96VP-CJYWM-3YT96-F4CFT-FP7VZ 33 K72P6-HM6RP-HHFFD-YH2P3-HKM6Z 34 DDQFK-6MYVC-CM337-WCWR7-RGF6Z 35 Y37DQ-X37DJ-JKCM4-QCD9J-PD7RZ 36 HT29J-YW2JP-9VVJ4-CDX7M-KTX9Z 37 9JPHV-7YT4K-D797J-JHMQX-PGMJZ 38 KH6WD-HV76Q-MXK7Q-GCFH7-9M46Z 39 727V2-X9VFQ-YQR4R-FGCKV-HMPVZ 40 6FMWK-3CJDQ-WMVKP-PH9Q2-CRD7Z
2017-12-04 06:19:16	paxful	Grizzled has marked this trade as paid. Waiting for seller to release bitcoins.
2017-12-04 06:19:36	Grizzled	40x$50
2017-12-04 11:58:41	rpstenangam	got it
2017-12-04 11:58:42	rpstenangam	wait me now
2017-12-04 14:50:36	Grizzled	ok
2017-12-05 05:57:26	Grizzled	Hi, when you can, let me know how long you need.
2017-12-05 06:05:26	paxful	Success! Seller has released bitcoins to buyers wallet.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Kvashuk engaged in dozens of transactions like the one shown above, resulting in his transfer of 5X5 codes collectively worth $7.8 million to several Paxful purchasers. At trial, the case agent will compare the codes shared in the chats with the codes purchased using the compromised test accounts, thus confirming that Kvashuk sold stolen test codes on Paxful and obtained Bitcoin through those sales. The case agent will also compare the codes in the Paxful chats with the spreadsheets and other records found in Kvashuk's home, further confirming that Kvashuk stole the CSV and re-sold it online. As the case agent will explain, Kvashuk often re-sold the gift cards at a discount of approximately 55%—*i.e.*, for every $1 of CSV that Kvashuk sold, he received approximately $0.55 in Bitcoin. That is because CSV sold in bulk has a somewhat depressed market value in part due to the fact that the CSV can only be used to purchase items on the Microsoft online store, whereas the currency used to purchase the CSV has more universal use.

3. Kvashuk's Conversion Of Bitcoin Into U.S. Dollars And Physical Assets

IRS SA Don Ellsworth, an expert in cryptocurrency, will testify about how Kvashuk transferred the Bitcoin he obtained on Paxful into a financial account in his own name on the cryptocurrency exchange Coinbase and other destinations. SA Ellsworth is expected to explain that cryptocurrency is a form of cryptocurrency that is entirely digital and de-centralized, insofar as it does not depend on the issuing authority of any government. Bitcoin is one cryptocurrency. Bitcoin can be stored in a centralized account with a cryptocurrency exchange that resembles a traditional investment account. It can also, however, be stored in digital "wallets" that are loaded on a person's digital device and unlocked using a password, much like traditional cash can be stored in a locked safe in somebody's residence. Every account or wallet for Bitcoin is assigned some version of a digital "address" that facilitates transactions between users. Agents found references to these types of "addresses" in the working notes found in Kvashuk's home.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Transactions involving Bitcoin can be traced, using specialized techniques, through the use of the Blockchain, an accumulating "chain" of blocks of digital data regarding Bitcoin transactions. As SA Ellsworth will explain, it is his expert opinion that approximately 72% of the Bitcoin that Kvashuk obtained on Paxful eventually was transferred into an account in Kvashuk's name at Coinbase, the cryptocurrency exchange. The remaining 28% of Paxful Bitcoin was transferred to a variety of different sources, some of which the IRS has been able to trace. In order to obscure the path of that Bitcoin, Kvashuk used so-called Bitcoin "mixers," which essentially mix Bitcoin from multiple different people before then disaggregating them again and sending the Bitcoin to their intended destinations. SA Ellsworth will describe mixers, and then show how Kvashuk used mixers to move millions into his Coinbase account. Had Kvashuk not taken steps to conceal the Blockchain record, he could immediately have been identified by Coinbase for transacting in massive amounts of Bitcoin from Paxful.

After receiving Bitcoin into his Coinbase account, Kvashuk converted that Bitcoin into U.S. dollars. Kvashuk used those proceeds as follows:

- Kvashuk's use of proceeds to purchase a waterfront home: Kvashuk used more than $1.6 million in criminal proceeds to purchase this waterfront home in Renton, Washington:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Records produced by Wells Fargo Bank N.A. ("Wells Fargo") and Fidelity Investments show that Kvashuk used assets from accounts at those financial institutions to make his earnest money deposit, make an additional payment, and then pay off the remainder of the home purchase in cash. As SA Hergert will explain, those records also show that the money in the Wells Fargo and Fidelity accounts originated in Kvashuk's Coinbase account (*i.e.*, the account into which he deposited Bitcoin that he obtained using the stolen CSV).

- Kvashuk's use of proceeds to purchase a Tesla: Kvashuk also used criminal proceeds to purchase a luxury car manufactured by Tesla: a new 2018 Tesla Model S P100DL.

Kvashuk's use of criminal proceeds to capitalize an investment account: Through his review of Kvashuk's account records, SA Hergert also found that Kvashuk transferred approximately $2.5 million into an account at Fidelity, which he used to purchase various securities. (As explained above, Kvashuk also used some of the money in the Fidelity account to purchase his home in Renton.)

B. *Kvashuk's Knowledge Of His Wrongdoing*

Kvashuk knew that his conduct was forbidden by Microsoft, and he therefore sought to conceal his role in it. In addition to the steps set out above (using other testers' accounts, using a phony name and address for the delivery of graphics cards he purchased, using a pseudonym on Paxful), Kvashuk took additional steps to try and hide his scheme.

First, Kvashuk used tools to anonymize his internet activity. An Internet Protocol ("IP") address is a numerical identifier that can be used to trace the origins of a computer's internet connections to a network, like a connection to Microsoft's online store. To conceal his IP address, Kvashuk used a service called "Private Internet Access" that re-routes connections through generic IP addresses.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Agents found "Private Internet Access" loaded on Kvashuk's digital devices, and the IP addresses used by the compromised test accounts traced back to PIA's service. A representative from the company that offers "Private Internet Access" will testify that their service anonymizes internet connections, because the company does not keep records of the IP addresses used by any particular subscriber. Because London Trust Media did not keep those types of subscriber records, investigators could not immediately determine, based solely on the IP addresses, whether it was Kvashuk or another London Trust Media user who connected to the Microsoft online store from the compromised UST accounts. As the government will explain at trial, Kvashuk's subscription to this internet anonymization service served as powerful evidence of his consciousness of guilt regarding the use of other testers' accounts to purchase CSV.

Second, although he admitted using the v-vokvas account to purchase CSV during his interviews with Microsoft investigators, Kvashuk made numerous materially false statements and omissions during those interviews that evidenced his consciousness of guilt.[4] Kvashuk claimed that he knew it was "not allowed" to trade CSV for cash, but omitted that he had purchased millions using the other testers' accounts. As set out above, Kvashuk also falsely assuaged the investigators that he had confronted his landlord about the deliveries to "Grigor Shikor," even though he had done no such thing.

Third, Kvashuk concealed the source of his income when dealing with tax preparers. In emails to two different tax preparers (one of those preparers prepared his 2018 federal income tax return and the other only provided him advice), Kvashuk claimed that his Bitcoin was a "gift" from his father. Kvashuk even filed a Form 3520 form (which he asked the tax preparer to prepare), which declared the Bitcoin as a gift.

[4] After identifying Kvashuk as a suspect, Microsoft investigators interviewed him on May 10, 2018 and May 18, 2018. Andy Cookson, the Microsoft investigator who conducted those interviews, will testify at trial. Mr. Cookson will testify that Kvashuk consented to the use of an audio recording device at both interviews. (Cookson's recording device ran out of batteries towards the end of the first interview, which caused the recording not to capture some portion of the interview.) At trial, the government will offer into evidence the audio recordings of the two interviews. Transcripts of the audio recordings will be provided to the jury, but will not be offered into evidence.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

C. Procedural History

Law-enforcement agents arrested Kvashuk on July 16, 2019. He has been detained since his arrest. The Grand Jury returned the Second Superseding Indictment on December 4, 2019. On December 9, 2019, Kvashuk entered pleas of not guilty.

Trial is scheduled for February 18, 2020. The government anticipates that its case-in-chief will last approximately five days.

II. AGREED STATEMENT OF THE CASE

The parties have agreed on the following statement of the case:

This is a criminal case. Defendant Volodymyr Kvashuk is accused of fraudulently obtaining over $10 million in digital gift cards from his employer, Microsoft Corporation. Kvashuk allegedly stole the identities of other Microsoft employees to improperly access Microsoft's computer system in order to steal the digital gift cards. Kvashuk allegedly resold the gift cards to third parties, and then used the proceeds in financial transactions, including the purchase of a house and a vehicle. Kvashuk allegedly failed to report income from the fraud on his federal income tax returns.

The United States has the burden of proving the charges beyond a reasonable doubt.

III. LEGAL ISSUES

A. Access Device Fraud

Count 1 of the Second Superseding Indictment charges Kvashuk with access device fraud under 18 U.S.C. §§ 1029(a)(5) and (c)(1)(A)(ii). To prove this offense, the government must establish the following elements: (1) with an access device issued to another person, the defendant knowingly effected transactions; (2) through such transactions, the defendant obtained at any time during a one year period a total of at least $1,000 in any thing of value; (3) the defendant acted with the intent to defraud; and (4) the defendant's conduct in some way affected commerce between one state and another state, or between a state of the United States and a foreign country. Ninth Circuit Model Jury Instruction 8.88.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The first element of this offense requires proof of an access device issued to another person. An "access device" is a "means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any thing of value." 18 U.S.C. § 1029(e)(1) (defining "access device"). As the Ninth Circuit has explained, the term "access device" "should be construed broadly to encompass innovative schemes perpetrated by criminals who use unauthorized information to defraud." *United States v. Sorensen*, 937 F.2d 614, at *2 (9th Cir. 1991) (unpublished).

The Microsoft online store login credentials for the sfwe2eauto and zabeerj2 accounts are "access devices" that had been issued to other people. *See United States v. Barrington*, 648 F.3d 1178 (11th Cir. 2011). The test accounts had been assigned to Kvashuk's colleagues, A.C. (sfwe2eauto) and Z.J. (zabeerj2). During his recorded interview, Kvashuk acknowledged that each member of the UST team had a test account designated for his or her use.

The access devices assigned to other UST members could be used to obtain CSV, a "thing of value." Kvashuk also "effected transactions" using the access devices, by using the access devices to make hundreds of purchases of 5X5 codes on the Microsoft online store website. Through the fraud, Kvashuk obtained at least $1,000 in a one year period; indeed, he obtained millions of dollars through his use of the sfwe2eauto and zabeerj2 accounts. Kvashuk's intent to defraud is evidenced by the facts described above, including his violation of Microsoft's prohibition against using the testing program for personal enrichment, his efforts to conceal his involvement in the scheme by using other testers' identities, and his use of internet-anonymization tools.[5]

Microsoft witnesses will testify that Kvashuk's conduct affected interstate or foreign commerce because the Microsoft online store operates in interstate and foreign commerce. CSV purchased on the Microsoft online store can be redeemed by purchasers

[5] Ninth Circuit Model Jury Instruction 5.12 defines "intent to defraud" to mean "an intent to deceive or cheat."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

all over the world. Indeed, Microsoft records show that Kvashuk purchased digital gift cards in various currencies, including U.S. dollars and Euro.

B. Unauthorized Access To A Protected Computer In Furtherance Of Fraud

Count 2 of the Second Superseding Indictment charges Kvashuk with access to a protected computer in furtherance of fraud in violation of 18 U.S.C. § 1030(a)(4) and (c)(3)(A). The elements of this offense are that: (1) the defendant knowingly accessed without authorization a computer used in or affecting interstate or foreign commerce; (2) the defendant did so with the intent to defraud; (3) by accessing the computer without authorization, the defendant furthered the intended fraud; and (4) the defendant by accessing the computer without authorization obtained anything of value. Ninth Circuit Model Jury Instruction 8.99.

The Microsoft online store operates on servers controlled by Microsoft, and it is available to purchasers all over the world. Its servers therefore are computers "used in or affecting interstate or foreign commerce," as the first element of the offense requires. As described above, Kvashuk acted with the intent to defraud and obtained something of value through his unauthorized access.

Kvashuk's knowing use of the sfwe2eauto and zabeerj2 accounts to access the Microsoft online store, to purchase CSV from the Microsoft online store was "without authorization," as the first element requires. *See United States v. Nosal ("Nosal II")*, 844 F.3d 1024, 1034-35 (9th Cir. 2015) (explaining that, for purpose of defining "without authorization," "'authorization' means 'permission or power granted by an authority") (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). Neither Microsoft nor Kvashuk's UST colleagues authorized his use of their accounts to access the Microsoft online store, or to purchase CSV from the store.

C. Mail Fraud

Count 3 of the Second Superseding Indictment charges Kvashuk with mail fraud, in violation of 18 U.S.C. § 1341.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The elements of this offense are that: (1) the defendant knowingly participated in or devised a scheme or plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, or promises; (2) the statements made or facts omitted as part of the scheme were material; that is, they had a natural tendency to influence, or were capable or influencing, a person to part with money or property; (3) the defendant acted with the intent to defraud, that is, the intent to deceive or cheat; and (4) the defendant used, or caused to be used, the interstate mails to carry out or attempt to carry out an essential part of the scheme. Ninth Circuit Model Instruction 8.121; *see also United States v. Woods*, 335 F.3d 993 (9th Cir. 2003). Here, the charged shipment is the graphics cards purchased by the xidijenizo account, which Federal Express shipped from Ontario, California to Seattle, Washington.

A scheme to defraud may be proven by evidence that the defendant sought to obtain money or property by false representations, deceitful statements, half-truths, or the concealment of material facts. *United States v. Beecroft*, 608 F.2d 753, 757 (9th Cir. 1979); *see also United States v. Allen*, 554 F.2d 398, 410 (10th Cir. 1977). "[T]he words 'to defraud' have the common understanding of wronging one in his property rights by dishonest methods or schemes and usually signify the deprivation of something of value by trick, deceit, chicane or overreaching." *Carpenter v. United States*, 484 U.S. 19, 27 (1987) (citations omitted).

The government need not prove a specific false statement was made. *See United States v. Woods*, 335 F.3d 993, 999 (9th Cir. 2003) ("Rather there are alternative routes to a . . . conviction, one being proof of a scheme or artifice to defraud, which may or may not involve any specific false statements."). Nor does the jury need to be "unanimous on the particular false promise" made during the scheme. *See United States v. Lyons*, 472 F.3d 1055, 1068 (9th Cir. 2007), *overruled on other grounds by United States v. Contreras*, 593 F.3d 1135 (9th Cir. 2010).

Here, the proof that Kvashuk devised a scheme is straightforward. Kvashuk stole CSV and converted it into U.S. dollars, real property, a car, and items that he purchased

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

on the Microsoft online store, all of which are "money or property." Kvashuk's scheme also relied on the use of material false and fraudulent pretenses, including but not limited to the following: First, he purported to participate in the UST testing program in pursuit of the program's intended purpose to test the operation of the Microsoft online store. In truth, and in contrast to those representations, Kvashuk used test accounts, including his own test account, to enrich himself. Second, he used other testers' identities to carry out the scheme by using their test accounts. Third, he used Grigor Shikor, a phony name, when purchasing and receiving the graphics cards he purchased using stolen CSV. Fourth, he used internet anonymization tools to conceal his true IP address, in order to make it appear as if his connections to the online store originated from locations other than his own residence.

The interstate mailing alleged in Count Three was a shipment that Microsoft sent from Ontario, California to Kvashuk's Seattle residence via Federal Express, a private and commercial interstate carrier. As set out above, Microsoft records show that Kvashuk used a Microsoft online store account registered under the email address xidijenizo@axsup.net to order a graphics card using CSV that he stole using the vokvas test account. When ordering the graphics card, Kvashuk directed Microsoft to ship it to a made-up name ("Grigor Shikor") at a made-up apartment (unit number 309) in his apartment building. Federal Express records show that the package was delivered in accordance with Kvashuk's instructions.

D. Wire Fraud

Counts 4 through 8 of the Second Superseding Indictment charge Kvashuk with wire fraud, in violation of 18 U.S.C. § 1343. The elements of this offense are: (1) the defendant knowingly participated in a scheme or plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, or promises; (2) the statements made or facts omitted as part of the scheme were material; that is, they had a natural tendency to influence, or were capable of influencing, a person to part with money or property; (3) the defendant acted with the intent to defraud; that is,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the intent to deceive or cheat; and (4) the defendant used, or caused to be used, an interstate wire communication to carry out or attempt to carry out an essential part of the scheme. Ninth Circuit Model Instruction 8.124.

The defendant need not have been aware of the interstate character of the wire communication sent in furtherance of the scheme. *See id.*; *see also United States v. Jinian*, 725 F.3d 964, 965 (9th Cir. 2013). Nor must the defendant have personally caused the wire transmission. *See United States v. Jones*, 712 F.2d 1316, 1320 (9th Cir. 1983). Rather, it is enough that the defendant knows that a wire will be used in the ordinary course of business or can reasonably foresee its use. *Id.*; *United States v. Lothian*, 976 F.2d 1257, 1262-63 (9th Cir. 1992). In addition, the wire communication need not itself contain a false representation to be in furtherance of a scheme to defraud. Instead, the government need only show that the communication was "incident to an essential part of the scheme." *Schmuck v. United States*, 489 U.S. 705, 711 (1989).

Each separate wire communication in furtherance of the scheme to defraud constitutes a separate violation of the wire fraud statute. *United States v. Vaughn*, 797 F.2d 1485, 1493 (9th Cir. 1986). Here, Kvashuk is charged with five separate wire communications in furtherance of his scheme to defraud, as set out in the following subsections:

1. Counts 4 and 5

Counts 4 and 5 arise out of emails from Microsoft Corporation to the email address mstest_avestu@outlook.com, which confirmed two purchases of $10,000 in CSV. As set out above, the avestu account was one of the UST accounts that Kvashuk used to purchase CSV. It had originally been registered under the email address mstest_avestu@outlook.com. As Microsoft records show, when the avestu account made purchases on the Microsoft online store, Microsoft sent a confirmation email to the registered email address. The email confirmed the purchases of the gift cards, and provided the 5X5 codes that could be used to redeem the gift cards' value. The emails

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

were incident to the purchase of CSV from the Microsoft online store, which plainly was an essential part of the scheme.

At trial, a Microsoft custodian will testify that the Microsoft servers that sent the emails were in Texas (Count 4) and California (Count 5), respectively. In turn, the server that received the emails sent to mstest_avestu@outlook.com was in Virginia, thus establishing that both emails traveled in interstate commerce. Although neither email traveled from or to the State of Washington, the government will offer location records found in Kvashuk's Google account in order to establish that he was in Washington State at the time he caused the emails to be sent.[6]

2. Counts 6 and 7

Counts 6 and 7 arise out of Kvashuk's electronic communications to Paxful regarding two transactions in which he negotiated the exchange of stolen CSV for Bitcoin. A Paxful custodian of records will testify about records which reflect that the communication concerned transactions that Paxful identified as "trade jW1DK8xP2m5" and "trade vMoJGaDB9mx" in which Kvashuk (using the screenname "grizzled") sold 5X5 codes to other users. In the relevant electronic communications, Kvashuk transmitted dozens of 5X5 codes to the counterparties in his two transactions. In order to establish the interstate character of the electronic communications, the government will admit (1) location data from Kvashuk's Google account, which shows that he was in Seattle at the time of both communications; and (2) the testimony of a Paxful custodian of records, which will establish that the Paxful servers to which Kvashuk sent the 5X5 codes were outside the State of Washington.

[6] Kvashuk's presence in Washington at the time he caused the interstate wires to be sent establishes that this District has venue over the offenses charged in Counts 4 and 5. As the Ninth Circuit has explained, "venue is established in those locations where the wire transmission at issue originated, passed through, or was received, or from which it was 'orchestrated'." *United States v. Pace*, 314 F.3d 344, 349-50 (9th Cir. 2002).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

3. Count 8

Count 8 arises out of an email from Kvashuk to his tax preparer regarding the preparation of his 2018 federal income tax return. In the email, Kvashuk claimed falsely that he received his Bitcoin holdings from his father, and thus omitted that he actually received the Bitcoin by selling stolen CSV. At the time he sent the email, Kvashuk was in Seattle and his tax preparer was in Illinois, rendering the email an interstate communication. As both Kvashuk's tax preparer and IRS revenue agent Shipley will testify, by claiming that he received the Bitcoin from his father, Kvashuk avoided having to declare that Bitcoin as income. Kvashuk also avoided having to disclose that the Bitcoin had been obtained through fraud.

E. Making And Subscribing To A False Tax Return

Counts 9 and 10 charge Kvashuk with making and subscribing to false tax returns, in violation of 26 U.S.C. § 7206(1). The elements of this offense, in the context of this case, are: (1) the defendant signed and filed a tax return for the years [2017 and 2018] that he knew contained false information as to a material matter; (2) the return contained a written declaration that it was being signed subject to the penalties of perjury; and (3) in filing the false tax return, the defendant acted willfully. Ninth Circuit Model Instruction 9.39. A matter is material if it had a natural tendency to influence, or was capable of influencing, the decisions or activities of the Internal Revenue Service. *Id.*

Kvashuk's federal income tax returns for the 2017 and 2018 tax years did not disclose any of the gains from his scheme. Rather, the income he reported in both 2017 ($114,103) and 2018 ($83,895) was substantially lower than his actual income during those two tax years. As IRS revenue agent Shipley will explain, those gains are taxable income despite the fact that they were criminally derived. As a result of Kvashuk's failure to report the substantial income that he received through his scheme, he avoided having to pay income taxes for both tax years.

In order to prove that Kvashuk acted willfully, the government must prove beyond a reasonable doubt that he knew federal tax law imposed a duty on him to report the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

income that he failed to report, and he intentionally and voluntarily violated that duty. Ninth Circuit Model Instruction 9.42. Here, Kvashuk's willfulness is evidenced by his emails to two different tax preparers in regard to the preparation of his 2018 federal income tax return. In both emails, Kvashuk claimed that his father had sent him his Bitcoin holdings. Kvashuk ultimately retained one of the tax preparers to compile and file his 2018 tax return on the basis of the false information he had provided.

Consistent with his false characterization of his criminal proceeds as money he received from his father, Kvashuk also filed a Form 3520, which declared his Bitcoin as a "gift" to the IRS. Kvashuk's tax preparer will testify that Kvashuk instructed him to prepare that form. By declaring his criminal proceeds to be a "gift," Kvashuk made clear that he understood that they otherwise would need to be declared as taxable income.

F. Money Laundering

Counts 11 through 16 charge Kvashuk with money laundering under 18 U.S.C. § 1957. The elements of this offense are that: (1) the defendant knowingly engaged or attempted to engage in a monetary transaction; (2) the defendant knew the transaction involved criminally derived property; (3) the property had a value greater than $10,000; (4) the property was in fact derived from specified unlawful activity; and (5) the transaction occurred in the United States. Ninth Circuit Model Jury Instruction 8.150.

The Second Superseding Indictment alleges that Kvashuk knowingly engaged in the following monetary transactions, each of which gives rise to a separate count of money laundering:

Count	Date	Transaction	Transaction Amount
11	June 1, 2018	Transfer from Fidelity account number ending in -9568 to Rainier Title for purchase of Renton property	$1,513,903.67
12	June 1, 2018	Transfer from Wells Fargo account number ending in -5789 to Rainier Title for purchase of Renton property	$113,993.28

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

13	March 20, 2018	Transfer from Wells Fargo account number ending in -5789 to Tesla for purchase of Tesla vehicle	$162,899.55
14	April 8, 2018	Transfer from Wells Fargo account number ending in -5789 to Fidelity account -9568	$990,000
15	March 2, 2018	Transfer from Coinbase account number ending in –ae58 to Wells Fargo account -5789	$492,550
16	April 3, 2018	Transfer from Coinbase account number ending in –ae58 to Wells Fargo account -5789	$473,810.44

Representatives from Wells Fargo and Fidelity Investments will testify that each of the alleged transactions were monetary transactions that occurred on the dates set out above. Indeed, each transaction involved the transfer of U.S. dollars between two financial institutions. *See* 18 U.S.C. § 1957(f)(1) (defining "monetary transaction"); *id.* § 1956(c)(5) (defining "monetary instruments").

The term "specified unlawful activity" includes mail fraud and wire fraud under 18 U.S.C. §§ 1341 and 1343. Each of the financial transfers set forth in the above table included more than $10,000 in proceeds from the scheme that gives rise to the charges of mail and wire fraud in Counts 3 through 8. In order to establish that the each transfer involved more than $10,000 in criminally derived proceeds, the government will elicit the testimony of SA Hergert and SA Ellsworth. SA Hergert and SA Ellsworth will testify that, at the time of each of the transfers set out above, the relevant bank balances included less than $10,000 in legitimate non-criminal proceeds. In order to conduct those monetary transactions, Kvashuk necessarily relied on criminally derived proceeds.

G. Aggravated Identity Theft

Counts 17 and 18 of the Second Superseding Indictment charge Kvashuk with aggravated identity theft, in violation of 18 U.S.C. § 1028A. The elements of this offense are: (1) the defendant knowingly transferred, possessed, or used without lawful authority a means of identification of another person; (2) the defendant knew that the means of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

identification belonged to a real person; and (3) the defendant did so during and in relation the crimes of access device fraud (as charged in Count 1) and unauthorized access to a protected computer (as charged in Count 2).[7] Ninth Circuit Model Jury Instruction 8.83.

Counts 17 and 18 arise out of Kvashuk's use of the sfwe2eauto and zabeerj2 accounts. Kvashuk filed a pretrial motion to dismiss these counts, arguing that corporate accounts could not constitute a "means of identification." Mot., Dkt. 66. The Court rejected that argument in its oral ruling at the first pretrial conference.

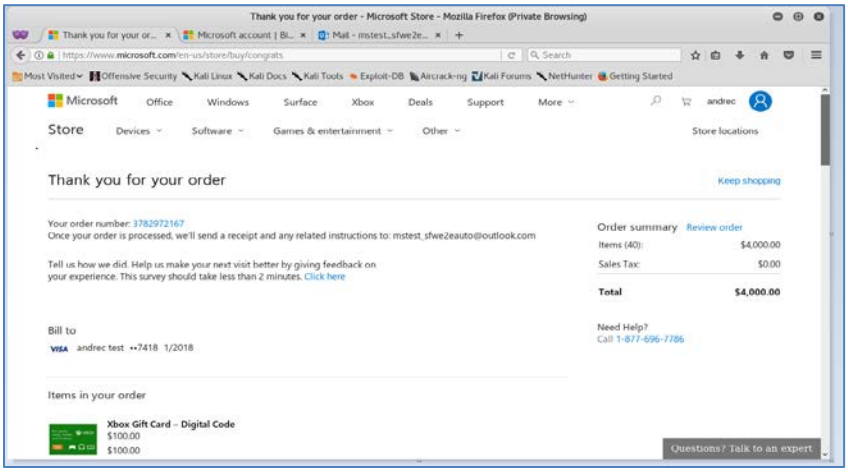
The usernames and passwords for the compromised UST accounts are "means of identification" under section 1028A because they identified specific individuals: A.C and Z.J. *See* 18 U.S.C. 18 U.S.C. § 1028(d)(7) (defining "means of identification" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual"); *see also United States v. Blixt*, 548 F.3d 882, 887 (9th Cir. 2008) ("By using the word 'any' to qualify the term 'name,' the statute reflects Congress's intention to construe an expansive definition."). As explained in the government's earlier briefing in this case, usernames and passwords for electronic accounts are "means of identification." *See Barrington*, 648 F.3d at 1193.

Kvashuk also knew that those means of identification belonged to real people. As set out above, during his interview with Microsoft investigators, he acknowledged that members of the UST team each had been assigned test accounts. Files found on Kvashuk's digital devices also confirm his knowledge that the compromised accounts had been assigned to real people within the UST team. For instance, the screenshot below, which was found on one of Kvashuk's digital devices, referred to a purchase made by the sfwe2eauto account. As shown in the screenshot, the billing information for the

[7] Access device fraud and unauthorized access to a protected computer are both crimes covered by 18 U.S.C. § 1028A(c).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

transaction referred to an internal credit card issued to "**andrec** test"—i.e., A.C., the UST member to whom the sfwe2eauto account had been assigned.



IV. Evidentiary Issues

A. Particular Hearsay Issues

1. Defendant's Statements

The government will offer certain statements made by Kvashuk. These statements are admissible as admissions of a party opponent. Fed. R. Evid. 801(d)(2)(A); *United States v. Burreson*, 643 F.2d 1344, 1349 (9th Cir. 1981). The government may offer all, some, or none of a defendant's statements at trial under Rule 801(d)(2). Defendant may not offer his own statements under this rule because they are not statements of the proponent's "party-opponent." *United States v. Ortega*, 203 F.3d 675, 682 (9th Cir. 2000) (party cannot offer his own statement as party admission). The government will offer evidence of Kvashuk's statements to Microsoft investigators during his May 10 and May 16, 2018 interviews, including statements in which he admitted using the v-vokvas account to purchase CSV and the safirion@outlook.com account to redeem that CSV, and in which he admitted that he knew it was not "allowed" to buy CSV with test accounts and to exchange that CSV for cash.

The government will also offer evidence of Kvashuk's statements in emails and online chats, some of which Kvashuk made under the cover of his "grizzled" username

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

on Paxful. Many of these statements are not offered for the truth of the matter asserted, and therefore do not constitute hearsay to begin with. Rather, they are simply offered to show Kvashuk's trading activity and his representations to third parties. If offered for the truth of the matter asserted (i.e., to attribute them to Kvashuk), the Court must make a preliminary finding pursuant to Federal Rule of Evidence 104 that proof has been introduced "sufficient to support a finding" that Kvashuk was the person who made the statements. Fed. R. Evid. 104(b).

The Ninth Circuit has held that the quantum of proof for this finding is the existence of "substantial evidence," which is a lower standard of proof than preponderance of the evidence. *United States v. Flores*, 679 F.2d 173, 178 (9th Cir. 1982). As discussed in the factual recitation above, there is more than "substantial evidence" that Kvashuk was the user of the email account that bore his own name and the Paxful account registered under the "grizzled" username. Accordingly, the Court should find pursuant to Rule 104 that these statements are admissible as party admissions.

2. Records of Regularly-Conducted Activity and Rule 902(11) Certifications

The government will offer records of regularly-conducted activities of businesses, including records of Microsoft, Google, Paxful, Coinbase, Wells Fargo, Federal Express, Fidelity Investments, Rainier Title, and Tesla. These records are admissible pursuant to Rule 803(6), which allows for admission of a record if it is made at or near the time of the events set forth therein, by a person with knowledge, and is kept in the course of regularly-conducted activity of a business or other organization, if it is the regular practice of the organization to make the record. Fed. R. Evid. 803(6).

Any person familiar with the record-keeping practices of the business is a sufficient foundational witness. Personal knowledge of the document is not required, and does not affect its admissibility. *United States v. Childs*, 5 F.3d 1328, 1334 (9th Cir. 1993) (the phrase "other qualified witness" is broadly interpreted to require "only that the witness understand the record-keeping system" at the particular organization). A record

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

generated by a third party and received and relied upon in the ordinary course, such as an invoice, becomes a business record of the company relying upon it. *Childs*, 5 F.3d at 1333-34; *see United States v. Jawara*, 474 F.3d 565, 585 (9th Cir. 2007) ("[W]e would have no trouble concluding that a college in the United States was a proper custodian of its' students' SAT results, even though the SAT results were actually prepared by another entity"). In determining whether these foundational facts have been established, the court may consider hearsay and other evidence not admissible at trial. Fed. R. Evid. 104(a).

The government intends to authenticate many of these business records by offering Rule of Evidence 902(11) certifications rather than live testimony. Rule 902(11) provides that a party may authenticate a business record through a signed certification of records custodian if the proponent of the evidence gives the adverse party adequate notice of its intent to offer the record and the defendant does not object.

The government has provided all 902(11)s to the defense, and has informed the defense of its intent to admit these records on the basis of those certifications. The government has not received any objections.

The business records covered by Rule 902(11) include emails found in Kvashuk's Gmail account and in the Microsoft email accounts under which the compromised UST test accounts had been registered. In addition to authenticating these records by means of a Rule 902(11) certification, the government will provide evidence that will be "sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). *See, e.g., United States v. Fluker*, 698 F.3d 988, 999-1000 (7th Cir. 2012) (finding that emails were properly authenticated through circumstantial evidence, including the content of the email itself); *United States v. Siddiqui*, 235 F.3d 1318, 1322-1323 (11th Cir. 2000) (finding that emails were properly authenticated through circumstantial evidence, including because the email address had been associated with the defendant). As set out above, there is extensive evidence establishing that the Gmail account that bears Kvashuk's name in fact is his email account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

B. Expert Testimony

1. Admissibility of Expert Testimony

Federal Rule of Evidence 702 governs the admission of expert testimony. It is based on the recognition that "an intelligent evaluation of the facts is often difficult or impossible without the application of specialized knowledge." Rule 702 Adv. Comm. Note. Rule 702 provides:

> If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

Fed. R. Evid. 702.

In the *Daubert* decision, the Supreme Court adopted a flexible test for determining whether to admit scientific expert testimony under Rule 702. *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 588 (1993). The Supreme Court later extended *Daubert* to apply to "technical or other specialized knowledge." *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 147 (1999). However, *Kumho Tire* rejected the proposition that the *Daubert* factors should be rigidly applied, stating instead that those factors "may or may not be pertinent in assessing reliability, depending on the nature of the issue, the expert's particular expertise, and the subject of his testimony." *Kumho*, 526 U.S. at 138. While *Daubert* directs trial courts to serve as "gatekeepers" by excluding testimony that is genuinely unreliable, the gatekeeper role "is not intended to serve as a replacement for the adversary system." Fed. R. Evid. 702 Adv. Comm. Notes (quoting *United States v. 14.38 Acres of Land*, 167 F.3d 155 (5th Cir. 1996)). Indeed, *Daubert* itself made clear that "vigorous cross examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence." *Daubert*, 509 U.S. at 595. Further, the Ninth Circuit has stated that Rule 702 should be "construed liberally," as a rule of inclusion and not of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

exclusion. *United States v. Hankey*, 203 F.3d 1160, 1168-69 (9th Cir. 2000) (expert testimony on gang activity properly admitted as specialized knowledge where expert had extensive personal observations of gangs; "Rule 702 works well for this type of data gathered from years of experience and special knowledge").

An expert's opinion may be based on materials that are not otherwise admissible under the Federal Rules of Evidence. *See* Fed. R. Evid. 703 ("An expert may base an opinion on facts or data in the case that the expert has been made aware of or personally observed. If experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject, they need not be admissible for the opinion to be admitted."); *see also United States v. W.R. Grace*, 504 F.3d 745, 763 (9th Cir. 2007); *First Nat'l Bank v. Lustig*, 96 F.3d 1554, 1556 (5th Cir. 1996) (explaining that expert may properly rely on inadmissible hearsay).

2. The Government's Expert Testimony

The government disclosed its expert testimony to the defense on August 2, 2019, and supplemented those disclosures on December 5, 2019. As the government noted in its disclosures, not all of the disclosed witnesses were necessarily going to offer expert testimony, but rather the government made broad disclosures in an abundance of caution.

In addition to the witnesses discussed elsewhere in this filing, the government intends to call translator Andrei Medvedev. Mr. Medvedev has been a Washington State court-certified interpreter since 2010 and has been an active court interpreter since that time, testifying at various levels of state and federal courts.

One of the government's exhibits is a Ukranian-language note found in Kvashuk's residence. Mr. Medvedev will testify that he created the translation of the note that the government seeks to admit into evidence, along with the original note.

A translation of an otherwise admissible document is admissible based on a qualified interpreter's testimony that the interpretation is accurate. *United States v. Khan*, 794 F.3d 1288, 1294 (11th Cir 2015) (trial court properly admitted translations that contained translator's bracketed notes explaining the meaning of certain passages).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Challenges to the accuracy of the translation do not go to their admissibility. *Id.* Rather, the defendant may challenge the interpretations on cross examination, or by offering his own translation, "thereby allowing the jury to make the final decision as to which translation it [finds] most credible." *Id.* The government has proposed a limiting instruction based on the one approved by the *Shah* court, which instructs the jury that it should assess for itself whether the translation is accurate based on factors such as the qualifications of the translator.

C. Charts and Summaries

The government will offer various charts and other summaries of voluminous evidence. The charts and summaries will relate to Microsoft's business records that show CSV purchases by Kvashuk's vokvas account and the three other UST test accounts that he compromised.

The government also intends to offer charts that summarize Kvashuk's transactions on Paxful, in order to show (a) the total amount of CSV he sold on Paxful, (b) the total amount of Bitcoin he acquired, and (c) the close temporal relationship between those Paxful transactions, the CSV purchases made by the Microsoft test accounts, and deposits into Kvashuk's account at Coinbase. The government's charts and summaries will also address voluminous financial records from Kvashuk's financial accounts at Coinbase, Wells Fargo, and Fidelity Investments, including to show that the alleged acts of money laundering necessarily involved more than $10,000 in criminal proceeds.

These charts and summaries are admissible under Federal Rule of Evidence 1006, which provides in pertinent part that "[t]he contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation." Fed. R. Evid. 1006. "The purpose of the rule is to allow the use of summaries when the documents are unmanageable or when the summaries would be useful to the judge and jury." *United States v. Rizk*, 660 F.3d 125, 1130 (9th Cir. 2011). Summary evidence is admissible if the underlying materials upon

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

which the summary is based (1) are admissible in evidence; and (2) were made available to the opposing party for inspection. Fed. R. Evid. 1006; *Rizk*, 660 F.3d at 1130. The availability requirement ensures that the opposing party has an opportunity to verify the reliability and accuracy of the summary prior to trial. *Rizk*, 660 F.3d at 1130. The government provided all of the information underlying the summaries to the defense well in advance of trial.

D. Demonstrative Exhibits

The government may also use demonstrative charts during its opening statement, examinations of witnesses, and in closing argument. Such charts are permissible to assist the jury in understanding the evidence, even if they are not themselves admissible. *United States v. Stephens*, 779 F.2d 232, 238 (5th Cir. 1985) (approving simple flow charts tracing the defendant's use of loan proceeds).

The jury should be told the charts are presented as a matter of convenience and if found to be inaccurate they should be disregarded entirely. *United States v. Abbas*, 504 F.2d 123, 125 (9th Cir. 1974). The government suggests that the Court instruct the jury using Ninth Circuit Model Instruction 4.15, which contains this cautionary language.

E. Redaction of Personally Identifying Information

Local Criminal Rule 49.1 provides for the redaction from exhibits of certain information, including home addresses and "financial accounting numbers." Given the importance of financial account information in this case, the government will move to seal those records, rather than redact them. With respect to the address of the Renton waterfront home, this is a central piece of evidence in the case and is directly tied to the proof of several charged offenses. Accordingly, the government seeks leave of the Court to offer exhibits containing that address in unsealed and unredacted form.

F. Redaction of Information Relevant to Kvashuk's Asylum Application

At the initial pretrial conference, the Court barred the defense from introducing evidence related to Kvashuk's immigration status or pending asylum claim. Minute

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Entry, Dkt. 75. The government will redact references to Kvashuk's asylum application in its proposed trial exhibits.

V. Criminal Forfeiture

The United States intends to seek forfeiture in this case and provided notice to the Defendant of this intent in the initial, superseding, and second superseding Indictments (Dkt. Nos. 14, 49 & 61).

Specifically, the United States seeks to forfeit the following three items of property:

1) a Tesla vehicle, VIN No. 5YJSA1E40JF249750, Washington license plate no. BJW9291, registered to the Defendant in Renton, Washington;
2) all securities-invested funds held in the Fidelity Money Market Portfolio – Class I contained in Fidelity account number ending in -9568, held in the Defendant's name; and,
3) the real property located at 6409 Ripley Lane SE, Renton, Washington, titled in the Defendant's name.

There are multiple legal bases for forfeiting this property, as follows:

1) it constitutes or is traceable to proceeds of the Defendant's commission of Access Device Fraud (as alleged in Count 1 of the second superseding Indictment), or it facilitated that offense, and is therefore forfeitable pursuant to 18 U.S.C. § 982(a)(2)(B) and 18 U.S.C. 1029(c)(1)(C);
2) it constitutes or is traceable to proceeds of the Defendant's commission of Access to a Protected Computer in Furtherance of Fraud (as alleged in Count 2), or it facilitated that offense, and is therefore forfeitable pursuant to 18 U.S.C. § 982(a)(2)(B) and 18 U.S.C. 1030(i);
3) it constitutes or is traceable to proceeds of the Defendant's commission of Mail Fraud (as alleged in Count 3) and is therefore forfeitable pursuant to 18 U.S.C. § 981(a)(1)(C), by way of 28 U.S.C. § 2461(c);

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

4) it constitutes or is traceable to proceeds of the Defendant's commission of Wire Fraud (as alleged in Counts 4 – 8) and is therefore forfeitable pursuant to 18 U.S.C. § 981(a)(1)(C), by way of 28 U.S.C. § 2461(c); and,

5) it constitutes property involved in the Defendant's commission of Money Laundering (as alleged in Counts 11 – 16), or it constitutes proceeds of that offense, and is therefore forfeitable pursuant to 18 U.S.C. § 982(a)(1).

The United States expects the evidence at trial to establish the required nexus between each item of property and the identified offenses.

A. **Legal Standard for Forfeiture**

Criminal forfeiture is a form of punishment that is imposed as part of a criminal sentence. *Libretti v. United States*, 516 U.S. 29, 39 – 40 (1995). For the government to criminally forfeit property, there must be a predicate criminal conviction, a statute authorizing forfeiture for the crime of conviction, and evidence to support the statutorily required nexus between the property and the crime of conviction. *See e.g., United States v. Garcia-Guizar*, 160 F.3d 511, 518 – 20 (9th Cir. 1998) (reviewing these requirements). With respect to the required nexus, the government must establish the forfeitability of the relevant property by a preponderance of the evidence. *United States v. Martin*, 662 F.3d 301, 307 (4th Cir.2011); see also *United States v. Rutgard*, 116 F.3d 1270, 1293 (9th Cir. 1997); *United States v. Hernandez-Escarsega*, 886 F.2d 1560, 1576-77 (9th Cir. 1989). In other words, depending on the relevant forfeiture statute, the government must present evidence that establishes the relevant property is, "more likely than not," forfeitable as *proceeds* of the crime, property that *facilitated* the crime, and/or property *involved in* the crime. This lower standard of proof "is constitutional because the criminal forfeiture provision does not itself describe a separate offense, but is merely an 'additional penalty' for an offense that must be provide beyond a reasonable doubt." *United States v. Garcia-Guizar*, 160 F.3d at 518 (citing *United States v. Hernandez-Escarsega*, 886 F.2d at 1577).

In this case, there is statutory authority to forfeit the identified property following the Defendant's conviction on any one of the following charges: Access Device Fraud

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(Count 1), Access to a Protected Computer in Furtherance of Fraud (Count 2), Mail Fraud (Count 3), Wire Fraud (Counts 4 – 8), and Money Laundering (Counts 11 – 16). The United States expects the evidence at trial will establish, to a preponderance, that the identified property is *proceeds* of, *facilitating property* for, and/or property *involved in* the relevant offense (depending on the particular nexus required for the offense).

B. **Forfeiture Process**

Rule 32.2 sets out the procedures for determining the forfeitability of property in a criminal case. Forfeitures are decided after a guilty verdict is returned on a count that supports the forfeiture. *See* Rule 32.2(b)(1)(A). At that juncture, the specific question for the fact finder is "whether the government [has established the] requisite nexus between the property and the offense." Rule 32.2(b)(1)(A). The defendant and the government have a right for a jury to determine the forfeitabilility of any specific property.[8] This is not a constitutional right. *See United States v. Libretti*, 516 U.S. 29, 49 (1995) ("the nature of criminal forfeiture as an aspect of sentencing compels the conclusion that the right to a jury verdict on forfeitability does not fall within the Sixth Amendment's constitutional protection"). Instead, it is a right afforded by the rules governing criminal forfeiture. *See* Rule 32.2(b)(5) (providing the jury must determine the forfeitability of specific property if "either party" so requests).

As forfeiture is determined post-conviction, and is considered part of sentencing, the rules of evidence do not strictly apply to forfeiture proceedings. *See e.g.*, *United States v. Hatfield*, 795 F. Supp.2d 219, 229-30 (E.D.N.Y. 2011) (holding neither the Federal Rules of Evidence nor *Daubert* apply to forfeiture hearings) and *United States v. Creighton*, 52 Fed. Appx. 31, 35-36 (9th Cir. 2002) ("hearsay evidence is permissible at sentencing and does not, *per se*, lack sufficient indicia of reliability"). The Court may

[8] There is no right, however, for a jury to determine the forfeiture of a money judgment. *See* Rule 32.2(b)(1)(A) ("If the government seeks a personal money judgment, the court must determine the amount of money that the defendant will be ordered to pay."). The United States is not seeking forfeiture of a money judgment in this case, only forfeiture of the specific property identified above.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

consider any evidence that is "relevant and reliable." Fed. R. Crim. P. 32.2(b)(1)(B). This includes any evidence presented by the parties during trial on the substantive criminal offenses. *See id.* ("The court's [or jury's forfeiture] determination may be based on evidence already in the record …."); *see also United States v. Newman*, 659 F.3d 1235, 1244-45 (9th Cir. 2011) (same).

If the Defendant is convicted of one or more of the identified offenses, the United States expects to present the forfeiture case in a supplemental proceeding pursuant to Fed. R. Crim. P. 32.2(b)(1). The United States is willing to waive its right to retain the jury for that proceeding and have the Court decide the forfeitures. *See* Fed. R. Crim. P. 32.2(b)(5). If, however, the Defendant is unwilling to waive, the United States is prepared to present the forfeiture case to the jury. For use in that proceeding, the United States is submitting proposed forfeiture jury instructions and a special forfeiture verdict form.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In the forfeiture proceeding, the United States expects to rely entirely on the testimony and evidence introduced during the guilt/innocence phase of trial. The United States expects to present argument with respect to the forfeiture of the identified property, but it does not expect to present any additional testimony or exhibits. The United States reserves its right, however, to offer alternative arguments and evidence in support of forfeiture, and to take different positions with respect to forfeiture, as necessary to respond to developments at trial.

DATED this 7th day of February, 2020.

Respectfully submitted,

BRIAN T. MORAN
United States Attorney

s/Siddharth Velamoor

MICHAEL DION
SIDDHARTH VELAMOOR
Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
Telephone: (206) 553-7970
Fax: (206) 553-0755
E-mail: siddharth.velamoor@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on February 7, 2020, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant(s).

/s/ Siddharth Velamoor
SIDDHARTH VELAMOOR
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-3903
Telephone: (206) 553-2520
Fax: (206) 553-4440